College of Europe
Collège d'Europe

Brugge

Natolin

Guardian of the Galaxy?

Assessing the European Union's International Actorness in Cyberspace

Constant Pâris

DEPARTMENT OF EU INTERNATIONAL RELATIONS AND DIPLOMACY STUDIES

EU Diplomacy Paper 01/2021

College of Europe
Collège d'Europe
Brugge
Natolin

Department of EU International Relations and Diplomacy Studies

EU Diplomacy Papers

1/2021

Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace

Constant Pâris

Dijver 11 | BE-8000 Bruges, Belgium | Tel. +32 (0)50 477 251 | Fax +32 (0)50 477 250 | E-mail ird.info@coleurop.be | www.coleurope.eu/ird

About the Author

Constant Pâris is a French alumnus from the College of Europe in Bruges, where he obtained an MA in EU International Relations and Diplomacy Studies in 2020. He also holds an MA in European Governance from the Institut d'Études Politiques of Grenoble and Maastricht University, and a BA in Economics. He has previously worked at the French Ministry of Health, at the European Court of Justice for Judge Fredrik Schalin in Luxembourg, at the Institut pour la Démocratie in Paris, and as a research assistant in cybersecurity for the Centre d'Études sur la Sécurité Internationale et les Coopérations Européennes in Grenoble. This paper is based on his Master's thesis at the College of Europe (Hannah Arendt Promotion).

Dijver 11 | BE-8000 Bruges, Belgium | Tel. +32 (0)50 477 251 | Fax +32 (0)50 477 250 | E-mail ird.info@coleurope.eu | www.coleurope.eu/ird

Abstract

This paper aims at demystifying the international actorness of the European Union (EU) in cyberspace by assessing the extent to which the EU possesses sufficient capabilities to become a global cyber-power. For this purpose, the analysis relies on a kinetic approach based on the evaluation of four intertwined criteria: it first assesses the domestic features of the EU's cyber-actorness (resilience and coherence) to be able to further determine the characteristics of the EU's international cyber-actorness (attractiveness and responsiveness). The presence of both domestic criteria constitutes a fertile ground to assess the EU's actorness externally.

The paper argues that the EU has evolved from an inward-looking cyber-actor to a globally-oriented one. Internally, the EU has proved to be resilient, leading to the emergence of a 'collective cyber-securitisation' at the pace of cyber-attacks. Moreover, the EU has spontaneously leant towards a decentralised 'asymmetric governance' to overcome internal pitfalls such as national resistance linked to sovereignty issues. On the international stage, torn between a proactive and a reactive approach, the role of the EU as a cyber-actor is still blurred. Through a dense network of partnerships and international 'magnetism', the EU is shaping a 'collective immunity' in cyberspace by projecting its vision, norms, and values abroad. However, the EU's international actorness remains imbued with a 'paradoxical sleep': the brain acts, but the body is asleep.

The main conclusion is that the EU has become a budding global cyber-player that remains paralysed by its own inherent paradoxes and internal stalemates. Devoid of means to fulfil its global ambitions, the EU's 'cyber-power' remains limited to the regional scope. The EU is not yet a 'Guardian of the Galaxy' in cyberspace, but it does have the potential to become a globally influential and effective cyber-power if it manages to overcome its *sui generis* schizophrenic nature provoked by the tensions between its national and supranational levels.

Introduction: cyberspace, a known unknown world to rule for the EU

In an increasingly interconnected world, cyberspace has emerged as a complex and multidimensional arena. Rooted in the rapid pace of technological developments, new borderless security challenges have emanated from this recent phenomenon and they have been escorted by a constellation of fast-evolving threats. The digital era is paradoxical: the more advanced and digitalised states become, the more exposed and vulnerable they are to a growing number of malicious state and non-state cyber-actors.[1]

In recent years, 'cyber-hysteria' has spread to inter-state competition and geopolitics.[2] Cyberspace has become a contested area where stakeholders with divergent visions fight to rule it, and it is now "used by states as an equaliser for levelling the geopolitical playing field".[3] Given the fast proliferation of transnational and innovative threats, cyber-concerns became a strategic security priority for the European Union (EU). In 2016, the EU Global Strategy (EUGS) proclaimed: "The EU will be a forward-looking cyber-player".[4] Four years later, where does the EU stand?

This paper aims at demystifying the international actorness of the EU in cyberspace in order to ascertain how 'cyber-capable' the EU is and to highlight the particular hindrances faced by the EU in its quest for 'global power'.[5] The analysis assesses the EU's capabilities, credibility and legitimacy in cyberspace. However, the paper does not aim to assess the effectiveness: the EU could be a 'Guardian of the Galaxy', that is a capable global cyber-power, but this does not automatically mean that the EU is an effective actor. By examining the EU's 'cyber-actorness', the paper aims to understand what type of cyber-capabilities an international actor would need in this era of hybrid threats. The research question underpinning this paper is thus the

---

[1] J. Limnell, "Russian cyber activities in the EU", in N. Popescu & S. Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018, p. 72.

[2] N. Pospecu & S. Secrieru, "Conclusions", in N. Popescu & S. Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018, p. 115.

[3] P. Pawlak & T. Biersteker, *Guardian of the Galaxy. EU cyber sanctions and norms in cyberspace*, Chaillot Paper, no. 155, European Union Institute for Security Studies, Paris, October 2019, p. 4.

[4] European External Action Service, *Shared Vision, Common Action: a Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*, June 2016, p. 42.

[5] In this study, 'actor' and 'power' are not used interchangeably. The paper assumes that the EU is a cyber-actor and could be called a cyber-power if it becomes a very capable actor in cyberspace.

following: to what extent does the EU possess sufficient capabilities to become a global cyber-power?

The main argument is that the EU is a budding global cyber-power because it has the capabilities and the potential to become global cyber-power but remains hampered by its own inherent paradoxes and constraints that impede it from achieving all of its ambitious goals. For instance, the EU is torn by tenacious divergences among its member states that are not disposed to give too much power to Brussels. It is also constrained to adopt asymmetrical approaches or limited to the function of a mere mediator in cyberspace.

The next section sets out the framework of analysis, followed by an overview of the evolving security environment and the cyber-threats this involves. The subsequent part, covering the EU's 'resilience' and 'coherence', explores the EU's domestic 'collective cyber-securitisation' and 'asymmetric governance' in cyberspace. This is then followed by an 'investigation of the EU's 'attractiveness' and 'responsiveness' to assess the international projection of the EU in cyberspace. The conclusion summarises the findings and offers potential avenues for further research.

Framework of analysis

The EU's cyber-policy can be differentiated across three areas: networks and information systems (NIS), cybercrime and cyber-defence.[6] According to the EU Agency for Cybersecurity (ENISA), cybersecurity can be defined as "compris[ing] all activities necessary to protect cyberspace, its users, and impacted persons from cyber-threats".[7]

This paper adapts the concept of 'actorness' from Bretherton and Vogler's definition to fit with the cyber-domain. 'Cyber-actorness' stems from the combination of three interrelated components: the external cybersecurity environment connotes the existence of an opportunity; cyber-actorness is further determined by the capabilities of the EU (internal abilities to exploit); and by the EU's presence (potential to project influence abroad).[8]

[6] G. Christou, "The collective securitisation of cyberspace in the European Union", *West European Politics*, vol. 42, no. 2, 2018, p. 281.
[7] ENISA, *Overview of cybersecurity and related terminology*, September 2017, p. 6.
[8] C. Bretherton & J. Vogler, *The European Union as a Global Actor*, London, Routledge, 2nd edn., 2006, pp. 12-61.

More specifically, the analysis draws together existing insights on cyber-actorness into a framework of analysis constituted of four criteria which help to determine the capabilities of the EU as an international cyber-actor. Settled into a two-level kinetic process, these variables are interdependent: domestic capabilities (resilience and coherence) are considered as a pre-requirement to ensure the possibility to exert external capabilities (attractiveness and responsiveness).

Resilience reflects the capability to "withstand, adapt and quickly recover from [...] shocks".[9] It will be assessed through the scouring of EU legal documents and strategies. The main argument is that cyber-crises have been a major driver for positive changes in EU narratives, EU policy-making, EU architecture, and EU norms.

Coherence, in terms of vertical coherence, connotes the capability to demonstrate cohesion and coordination between the European and national levels. The main argument is that whereas the primary responsibility for cybersecurity lies with the national governments, which may result in fragmentation, the EU remains the most efficient framework for addressing cyber-threats.

Attractiveness is the capability to arouse interest in building international cooperation, to spread norms and values, and *in fine* to gain consideration. The main argument is that the EU is 'immunising' cyberspace through a dense network of partnerships and by building resilience in third countries.

Responsiveness is defined as the capability to counter, deter and respond to cyber-attacks. The main argument is that in spite of having an ambitious sanctions regime, the EU is still hindered by serious constraints such as the challenge of attribution or divergences among its members, and is limited to act only as an international mediator. Consequently, the lack of responsiveness overburdens the EU's overall cyber-actorness on the international stage.

Deeply intertwined, these criteria form the basis of a step-by-step approach. Each criterion encompasses one argumentative assessment and carries the same relative weight. The analysis relies on one major assumption: the stronger each criterion, the more likely the EU may become a powerful global cyber-player. Consequently, the final assessment relies on how each criterion does impact the EU's global power in cyberspace.

[9] European Commission & High Representative, *A Strategic Approach to Resilience in the EU's External* Action, JOIN(2017) 21 final, Brussels, 7 June 2017, p. 3.

The evolving global security environment – e-trends: cyber is the new black

The dark side of the web: the cyber-threat landscape in Europe and beyond

Over a span of years, the global security environment has been deeply disturbed by a raise in transnational hybrid threats using cyber-means in a conventional conflict. The combination of domestic vulnerabilities and external pressures has pointed out the extent to which cyber-attacks can dramatically impact the proper functioning of states.[10] This new configuration has fashioned cyberspace as an international theatre of tensions. In 2019, the world has known an "unprecedented level of state-run operations in cyberspace, driven by broader geopolitical considerations".[11] Recent reports have estimated that by 2027 "the global demand for offensive cyber-systems is expected to rise by 39%".[12] At home and abroad, the EU's interests have been challenged by a series of cyber-operations led by state and non-state actors. These multifaceted threats have provoked a profound shift in how cyberspace is approached by the EU, conscious that its 'good governance' appears vital to ensure national, regional, and international security.

The cyber-attack against Estonia in 2007 is known as the world's first cyber-offensive targeting the entire digital infrastructure of an EU member state.[13] More recently, criminals targeted the information systems of European structures dealing with defence or foreign affairs.[14] Cyber-tools were also used to disrupt national elections making the risk of cyber-enabled meddling in internal political processes real.[15] In 2017, two worldwide state-sponsored cyber-attacks ('WannaCry' and 'NotPetya') deeply affected the very heart of numerous European national entities. They showed that governmental actors are "both able and willing to undertake malicious cyber-activities for political, economic or security gains".[16] Cybersecurity breaches have also

[10] P. Pawlak, "Protecting and defending Europe's cyberspace", in N. Popescu & S. Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018, p. 105.
[11] Pawlak & Biersteker, *op. cit.*, pp. 3-4.
[12] P. Pawlak, E. Tikk & M. Kerttunen, "Cyber Conflict Uncoded – The EU and conflict prevention in cyberspace", *Conflict Series Brief*, no. 7, European Union Institute for Security Studies, Paris, April 2020, p. 6.
[13] K. Ruus, "Cyber War I: Estonia Attacked from Russia", *European Affairs*, vol. 9, issue 1-2, 2008.
[14] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 105.
[15] Limnell, *op. cit.*, p. 71.
[16] E. Moret & P. Pawlak, *The EU Cyber Diplomacy Toolbox: towards a cyber-sanctions regime?*, Brief, no. 24, European Union Institute for Security Studies, Paris, July 2017, p. 1.

occurred against EU bodies, demonstrating that, far from being sheltered, the EU might be a privileged target. This evidenced the backwardness in the EU's cybersecurity.[17]

Cyber-attacks targeting Georgia, Ukraine or countries in the Western Balkans aspiring to join the EU or the North Atlantic Treaty Organisation (NATO) also alerted the EU of the potential risks of destabilising its neighbourhood. These attacks have "undermined democratic institutions, caused great economic loss and damaged critical infrastructures".[18]

Assessment: the Phantom menace of cyberspace

The first decade of the 21st century illustrated that "cyber-conflicts were becoming commonplace around […] Europe".[19] Highlighting the EU's deep vulnerabilities, cyber-threats and their potential wide-ranging consequences have led to urgency in political debates. Rather than a mere technological challenge, building cyber-resilience became a political task.[20] It forced European leaders to actively develop adequate responses while minimising the negative impact of cyber-attacks.

The following section focuses on how the EU adapted its behaviour and laid the foundations for shaping governance in this realm to best address them (resilience criterion). Then, the analysis zooms in on one level lower to assess whether member states are in line with the EU's approach, both in terms of rationale and practices (coherence criterion).

Resilience as the backbone of the EU's collective securitisation in cyberspace

The EU's policy on cybersecurity has been triggered by both cyber-trends and imminent crises. Threat perceptions have shaped Brussels' discourses and the challenge of securing cyberspace has risen up on the political agenda. [21] Consequently, a large range of legal instruments and tools snowballed into the EU while new structures were either set-up or fortified.

---

[17] H. Krause, "How to advance European cybersecurity?", *International Centre for Defence and Security, Estonia*, 8 June 2018.
[18] P. Pernik, "The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine", in N. Popescu & S. Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018,p. 63.
[19] D. Giantas & A. Liaropoulos, *Cybersecurity in the EU. Threats, frameworks and future perspectives,* Working Paper, no. 1, Piraeus, Laboratory of Intelligence & Cyber-Security, September 2019, p. 11.
[20] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 103.
[21] Christou, *op. cit.*, p. 279.

The salience of cyber-threats in the EU's narratives

In the early 2000s, the EU's narratives were silent on the conceptualisation of cyberspace as a security space. In 2004, the EU for the first time used the term as a 'threat', when it realised that European critical infrastructures including Information and Communications Technology became vulnerable to cyber-terrorism.[22] The 2005 Council Framework Decision on Attacks Against Information Systems (AAIS) confirmed those concerns and stipulated that "attacks against information systems [… require] a response at the level of the EU".[23]

The 2007 Estonian shock gave governments a wake-up call about the potential impact of cyber-attacks on their national sovereignty. This watershed led to "a paradigm shift denoting the expansion of national security and defence into cyberspace".[24] Actors became focused on "how such attacks and threats might be addressed at EU level".[25] Cyber-issues were mentioned for the first time as strategic cross-sectorial challenges with an external dimension: "attacks against private or government IT systems in EU Member States have given [cybersecurity] a new dimension, as a potential new […] weapon".[26] The EU rapidly became aware of the 'cyber-paradox': "not only have […] digital technologies become even more central to our economies and societies, but their vulnerability has increased and the number and seriousness of attacks has magnified".[27]

The EU identified cybersecurity as a strategic objective in its 2010 Internal Security Strategy.[28] However, Brussels became conscious that tackling cyber-challenges required tailor-made strategies. Thus, the 2013 Cybersecurity Strategy (2013 EUCSS) identified five strategic priorities aimed at achieving effective policies that address cyber-threats.[29] The external dimension of cybersecurity flourished in unison with this internal strategy: tied to the promotion of European values, it called for a more active

[22] European Commission, *Critical Infrastructure Protection in the Fight Against Terrorism*, COM(2004) 702 final, Brussels, 20 October 2004, pp. 3-4.
[23] Council of the EU, "Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *Official Journal of the EU (OJ)*, L69, 16 March 2005, p. 67.
[24] Pernik, *op. cit.*, pp. 58, 60.
[25] European Parliament, *Resolution of 24 May 2007 on Estonia*, 2007/2567 (RSP), 27 May 2007.
[26] European Council, *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World*, S407/08, 11 December 2008, p. 5.
[27] Christou, 2018, *op. cit.*, p. 290.
[28] Council of the EU, *Internal Security Strategy for the EU: Towards a European Security Model*, March 2010.
[29] European Commission & High Representative, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final, Brussels, 7 February 2013, pp. 4-5.

EU international engagement. In the following years, official documents clearly highlighted the centrality of cybersecurity for the shaping of future EU action and insisted on its international dimension.[30] The 2016 EUGS framed cybersecurity as a key security component and reaffirmed the EU's intention to be a "forward-looking cyber-player".[31] After the 2017 'WannaCry' and 'NotPetya' crises, EU narratives focused on the destructive magnitude of cyber-attacks and on the need to build resilience. Hence, a new Cybersecurity Strategy updated the 2013 EUCSS in 2017 (2017 EUCSS). It embraces three objectives: achieving EU cyber-resilience, creating effective cyber-deterrence to reduce cybercrime, and strengthening international cooperation to promote cyber-stability.[32]

The EU became conscious that cyberspace is a multidimensional world whose features need to be adequately addressed. Cybercrime and cyber-defence were rapidly incorporated into the EU agenda. The EU recognised cybercrime as an "integral part of efforts to develop an overarching EU strategy to strengthen cybersecurity".[33] It also categorised it as one of its main priorities on its Political Agenda on Security 2015-2020.[34] However, the EU's reaction was not provoked by the precipitating events, but it was rather a response to an accumulation of crises forging an international trend, and overall prompted by the European Convention on Cybercrime adopted in 2001 (Budapest Convention). The first incursion of the concept of 'cyber-defence' in the EU's agenda and operations dates back to 2012. The 2017 EUCSS also called for the development of cyber-defence capabilities within the Common Security and Defence Policy framework.[35]

The growing proliferation of malicious cyber-players has deepened the EU's concerns.[36] Russia represents the main challenge within the EU, and a complex issue, given the ties of some member states with the country. The 'NotPetya' malware attacks and cyber-coercion against Estonia, Georgia and Ukraine demonstrated the Russian ability to manipulate the cyberspace to undermine states' power structures.

---

[30] A. Barrinha & H. Carrapico, "How coherent if EU cybersecurity policy?", *EUROPP Blog*, London School of Economics and Political Science, 2018.
[31] EEAS, EUGS 2016, *op. cit.*, p. 42.
[32] European Commission & High Representative, *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU*, JOIN(2017) 450 final, Brussels, 13 September 2017, p.
[33] European Commission, *Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, COM(2012) 140 final, Brussels, 28 March 2012, p. 3.
[34] European Commission, *The European Agenda on Security*, COM(2015) 185 final, Strasbourg, 28 April 2015.
[35] European Commission & High Representative, JOIN(2017) 450 final, *op. cit.*, p. 2.
[36] Pawlak & Biersteker, *op. cit.*, p. 76.

These cyber-offensives have spread amongst Europe a widely shared view that Russia poses the risk of cyber-warfare.[37] It led to a profound atmosphere of mistrust within the EU where Russia is intuitively considered as the 'usual suspect' at the origin of every cyber-attack conducted in Europe. EU policymakers commonly admit and the extensive scope and hazardousness of Russia's cyber-activities and condemn its behaviour.[38]

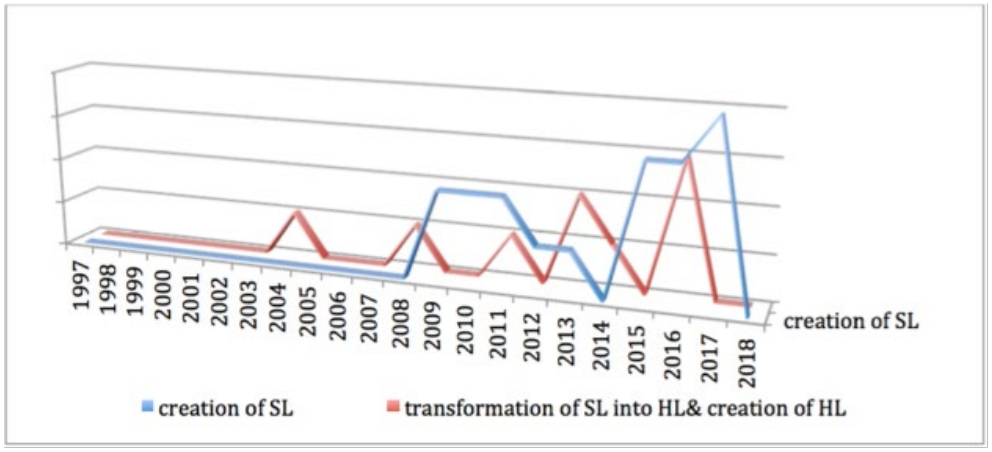
The proliferation and legalisation of cyber-related norms and structures

This section, combining a policy approach with legal analysis, scrutinises whether the transformation of narratives has been followed at the EU level by an alignment of policymakers and normative adjustments. Assessing the impact of crises on the development of EU cyber-related norms, it pictures cyber-attacks as a factor opening 'windows of opportunity' used by policy entrepreneurs to trigger a legalisation process, that is the transformation of soft law (SL) into hard law (HL), whose distinction "is determined by [...] the binding nature of the norm and the enforcement mechanism that ensures compliance with [it]".[39]

Throughout the 2000s, the EU relied on a soft law approach to regulate cyber-risks, symbolised by the emergence of non-legally binding EU documents and initiatives.[40]. Progressively, the body of EU norms relating to cybersecurity has grown.[41] Figure 1 traces the evolution of EU cyber-related norms over the last twenty years.

[37] Pernik, *op. cit.*, p. 57.
[38] Limnell, *op. cit.*, p. 68.
[39] S. Saurugger & F. Terpan, "Explaining the transformation of law. The cases of economic governance, migration and cybersecurity", Paper presented at the EUSA Conference, Denver, May 2019, pp. 2-3, 6.
[40] E. Fahey, "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation*, vol. 5, no.1, 2014, p. 49.
[41] R. A. Wessel, "Towards EU Cybersecurity law: regulating a new policy field", in N. Tsagourias & R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham: Edward Elgar Publishing, 2015, pp. 403-425.

Figure 1 – Evolution of soft and hard cyber-related norms



Source: Saurugger & Terpan, *op. cit.*, p. 15.

The 2007 cyber-attack against Estonia triggered an EU legalisation process and the adoption of preparatory acts in the following years.[42] The subsequent series of cyber-offensives throughout Europe and the related threat perceptions resulted in a parallel surge of soft norms. But it took time for the EU to adopt 'harder' legal instruments. Before 2013, the only case of hard law was the 2004 Council regulation creating ENISA and its revisions in 2008 and 2011. Since the 2013 EUCSS's objective of "achieving cyber-resilience" the EU is going through a period of greater legalisation.[43] Two main directives were adopted: the 2013 AAIS Directive, and the 2016 Networks and Information Systems Directive (the NIS Directive) which is "at the heart of the EU cyber-resilience and a cornerstone of the EU's effort to enhance its cybersecurity".[44] However, the influence of crises on the legalisation process seems less obvious. The 2007-08 cyber-attacks have triggered reactions followed by an affluence of EU initiatives, but time was required for these proposals to be converted into enforceable norms. The legalisation phase, symbolised by the adoption of the AAIS and NIS Directives, may be a result of the 2007-08 cyber-attacks, but if so, it is an indirect outcome.[45] Nevertheless, crises in third countries, especially in Ukraine since the annexation of Crimea' by the Russian Federation in 2014, might have led to the EU hardening its legal posture.

It seems that the stronger the crisis, the higher the probability of legalisation.[46] For instance, the 2017 peak of law creation might be explained as a reaction to the

[42] Saurugger & Terpan, *op. cit.*, pp. 27-28.
[43] Fahey, *op. cit.*, p. 49.
[44] Giantas & Liaropoulos, *op. cit.*, p. 18.
[45] Saurugger & Terpan, *op. cit.*, p. 32.
[46] *Ibid.*, p. 3.

gravity of the 'Wannacry' and 'NotPetya' attacks. The Cybersecurity Act, a regulation that entered into force in June 2019, reinforced ENISA's mandate and established an EU-wide cybersecurity certification scheme.[47] Later on, the Cyber Diplomatic Toolbox (Cyber-DT) set up the EU's cyber-sanctions regime.

The EU has over several years carefully drafted a '*cyber-acquis'* in response to crises.[48] Driven by the need to support this new legal framework and in its pursuit of resilience-building, the EU crafted appropriate structures for addressing cyber-issues. The creation, revamping or enhancement of cyber-specialised agencies – ENISA, the EU Computer Emergency Response Team (CERT-EU), Europol's European Cybercrime Centre (EC3) or the cyber branch of the European Defence Agency (EDA) – reflects the continuing EU adjustment to the insecure cyber-environment.

Assessment: the EU is an internal securitising actor in cyberspace

Cumulative cyber-threats have exposed member states' vulnerabilities and raised awareness amongst European leaders. Symbolised by the EUCSSs, the perception of growing risks induced "a securitisation move by authoritative EU institutional actors".[49] Consequently, the cyberspace has evolved into a mainstream security preoccupation while cyber-attacks have etched cyber-issues firmly onto the EU agenda. They acted as a catalyst for policy initiation, forcing the EU to make its approach to cybersecurity a more proactive. External pressures embodied an "impetus for the introduction of new security measures, the establishment of agencies and the formulation of a coordinated crisis response at the EU level".[50] This change coincided with the development of a legal framework with common guidance for member states to ensure that cyber-issues, framed as a collective threat, are tackled through norms.[51]

In the case of cybersecurity, the EU internal *modus operandi* was steadily adjusted at different points in time, both due to specific *ad hoc* emergencies and longer-term global trends. The incremental translation of EU narratives into concrete policies and legal initiatives shows a high degree of resilience. The EU has handled the challenges by sculpting a 'collective cyber-securitisation' within the European cyber-policy

[47] Council of the EU & European Parliament, "Regulation (EU) 2019/881 of 17 April 2019 on ENISA and on ICT cybersecurity certification", *OJ*, L151, 7 June 2019.
[48] Pawlak & Biersteker, *op. cit.*, p. 28.
[49] Christou, 2018, *op. cit.*, p. 286.
[50] Giantas & Liaropoulos, *op. cit.*, p. 30.
[51] Christou, 2018, *op. cit.*, p. 280.

space, as it has "justifie[d] its actions [...] by reference to an identified threat".[52] However, this capability to build resilience can only be effective if the EU is able to achieve success in internal cybersecurity governance.[53] To become an international cyber-power, the EU not only needs to show aptitudes in building cyber-resilience, but it must also be able to ensure coherence amongst its members. Admittedly, information exchange, cooperation and coordination are at the heart of resilience-building.

The following section assesses the 'coherence' criterion because "by acting in a co-ordinated fashion, the EU will be a stronger actor".[54]

The coherence conundrum: harmonisation or fragmentation?

The EU's appetite for coherence has been recognised by European narratives as being essential to tackle cyber-threats.[55] In practice, the EU has tried to construct vertical coherence through a 'communitarising process' aimed at steering member states to align with EU discourses, practices and values.[56] The dimension of vertical coherence evaluated here is twofold. First, it chimes with the existence among the actors of a shared understanding and situational awareness of what cybersecurity is and how it should be addressed.[57] Second, it reflects an institutional coordination which is determined by the "concrete practices of the actors involved in the cooperative efforts" and by the "incentives framing those relations".[58] However, a national resistance can be observed. The NIS Directive, considered as a milestone for the EU cybersecurity landscape, will be used as a case study.

Overall, while this section portrays some of the pitfalls that thwart the EU's quest for coherence, it also appraises the EU's internal governance in cybersecurity, meaning the ability to 'practice security' and overcome obstacles.

---

[52] J. Sperling & M. Webber, "The European Union: Security Governance and Collective Securitization", *West European Politics*, vol. 42, no. 2, 2018, p. 244.
[53] Giantas & Liaropoulos, *op. cit.*, p. 17.
[54] H. Carrapico & A. Barrinha, "The EU as a Coherent (Cyber)Security Actor?", *Journal of Common Market Studies*, vol. 55, no. 6, 2017, p. 1257.
[55] Carrapico & Barrinha, *op. cit.*, p. 1254.
[56] Christou, 2018, *op. cit.*, p. 282.
[57] Carrapico & Barrinha, *op. cit.*, p. 1256.
[58] *Ibid.*

'Europeanising' national approaches to cybersecurity: a success-story?

Acknowledging that "European cybersecurity remains almost exclusively a national prerogative" and aware of differences in member states' laws, the EU claims that cyber-issues are too complex to be left to the national level.[59] Consequently, it rapidly called for a "single EU voice on cybersecurity", with the intention of translating narratives into routinised practices.[60] The 2013 and 2017 versions of the EUCSS hammered home the necessity to forge a common approach among actors, instruments and policies[61] and portrays a 'cybersecurity community' across the EU institutions.[62]

The EU has reinforced its institutional apparatus and legal frameworks to make the member states converge towards common practices in order to counter cyber-threats in a more effective way.[63] Through the setting-up of agencies and competent authorities, the EU has pursued a constant improvement of coordination and cooperation. For instance, governments have been willing to concede an operational role to ENISA by strengthening its mandate.[64] However, the information-sharing hub lacks sufficient human and financial resources and seems limited to a mere supportive role.[65]

A common cyber-culture among EU member states?

In 2016, the EUGS pointed to the importance of fostering "a common cybersecurity culture".[66] Cyberspace is an emerging area particularly new to many EU member states, which may display different situational awareness and threat assessment.[67] The standardisation and terminology used between actors is essential to converge towards common priorities and to fashion adequate strategies in order to identify and address a threat. However, there is a lack of a collective understanding of the concept. Some member states have their own conceptualisations of cybersecurity,

[59] T. Renard, "The Rise of Cyber-Diplomacy: the EU, Its Strategic Partners and Cyber-Security", *ESPO Working Paper*, no. 7, European Strategic Partnership Observatory, June 2014, p.13.
[60] B. Fox, "Parliament demands single EU voice on cybersecurity", *EUObserver*, 13 June 2012.
[61] European Commission & High Representative, JOIN(2013) 1 final, *op. cit.*, pp. 5, 7, 10-12.; European Commission & High Representative, JOIN(2017) 450 final, *op. cit.*
[62] Carrapico & Barrinha, *op. cit.*, pp. 1260-1264.
[63] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 103.
[64] Christou, 2018, *op. cit.*, p. 286.
[65] Giantas & Liaropoulos, *op. cit.*, p. 18.
[66] EEAS, EUGS 2016, *op. cit.*, p. 22.
[67] P. Ivan, *Responding to cyber-attacks: prospects for the EU Cyber Diplomacy* Toolbox, Discussion Paper, European Policy Centre, 18 March 2019, p. 7.

while others still do not dispose of a clear meaning of the latter.[68] Furthermore, some governments are lagging behind in terms of shaping a national cyber-strategy despite cyber-attacks shedding light on their vulnerabilities. Neither cyber-incidents nor EU recommendations did spark among member states leaders an interest in adopting national policies or in putting forward an EU cybersecurity strategy.[69] After the attack against Estonia, only a handful of member states were separately developing cybersecurity strategies, while the first European documents on cyberspace were being issued. Only since the 2017 'WannaCry' attack, all member states have published they own cybersecurity strategies.[70]

Albeit, whilst member states' leaders "still conceive of cybersecurity as a private good to be dealt with through national strategies", they have progressively recognised the EU framework as pertinent to address transnational cyber-issues.[71] Member states have injected EU-related components into their own strategies, making coherence "directly connected with the perceived need for an EU-wide approach to cybersecurity".[72]

EU member states between compliance and resistance

Acknowledging the challenge of forging a common European strategy, the EU used its legal instruments to strengthen national strategies. Although the EU is able to produce hard legislation related to cyber-issues, member states are not always compliant when it comes to its implementation. The NIS Directive puts the emphasis on harmonising member states' capabilities and preparedness, but illustrates at the same time a lack of coherence and coordination troubles.[73]

The NIS Directive is the "first piece of European legislation that seeks to ensure a minimal institutional capability for reporting cyber-incidents across Member States".[74] It requires member states to be sufficiently equipped and to cooperate effectively among each other in order to boost the overall common level of NIS security in the EU

[68] K. F. Sliwinski, "Moving beyond the European Union's weakness as a cyber-security agent", *Contemporary Security* Policy, vol. 35, no. 3, 2014, p. 471.
[69] Giantas & Liaropoulos, *op. cit.*, p. 13.
[70] ENISA, *National Cyber Security Strategies – Interactive Map*, 2020.
[71] G. Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, Basingstoke, Palgrave Macmillan, 2016, pp. 171-189.
[72] Carrapico & Barrinha, *op. cit.*, p. 1261.
[73] *Ibid.*, p. 1266.
[74] Christou, 2018, *op. cit.*, p. 279.

and to avoid the fragmentation of practices.[75] Nonetheless, although all member states unanimously approved the text, some have been reluctant to grant the EU a more stringent control over their cyber-activities.[76] A majority of member states missed the target date (9 May 2018) to transpose the NIS Directive into their national legal frameworks.[77] Yet, cyber-crises might provoke the member states to incorporate new measures to enhance coherence within the EU. The 2017 'WannaCry' attack is considered as "the first ever case of cyber-cooperation at the EU level".[78] For the first time, national governments "exchanged information on a cybersecurity incident within the mechanism for operational cooperation under the NIS Directive".[79]

The case of Germany is particularly interesting. The country has always been disinclined "towards an evolution that could transfer excessively cybersecurity policies to EU institutions" and often tried to slow down the initiatives, but it fully transposed the NIS Directive before the deadline.[80] Thus, the lack of involvement from powerful countries does not impede the EU from a legal approximation of its cybersecurity policies. Additionally, some member states even offered a valuable contribution to the legalisation process, such as France, a "policy entrepreneur capable of building a coalition".[81]

Achieving coherence: a path fraught with pitfalls

EU member states might "suffer significant consequences of a cyber-attack due to their own negligence and failure to implement or transpose relevant EU legal frameworks and security recommendations".[82] Where does this resistance come from? While the EU's efforts are converging towards increasing coherence among its members, its main features are still hindered by a number of constraints.

First, as cyber-issues are linked to sovereignty, some member states remain sceptical towards an EU involvement and a collective vision on cybersecurity.[83] Cybersecurity is

[75] T. Renard & A. Barrinha, "The EU as a partner in cyber-diplomacy and defence", in J. Rehrl (ed.), *Handbook on Cybersecurity*, Vienna, Ministry of Defence of Austria, 2018, p. 187.
[76] Carrapico & Barrinha, *op. cit.*, p. 1267.
[77] P. Teffer, "EU countries miss cybersecurity deadline", *EU Observer*, 30 July 2018.
[78] ENISA, *WannaCry Ransomware: first ever case of cyber cooperation at EU level*, Press release, 15 May 2017.
[79] Council of the EU, *Cybersecurity – Information from the Commission*, 9621/17, Brussels, 31 May 2017, p. 1.
[80] Saurugger & Terpan, *op. cit.*, p. 31.
[81] *Ibid.*
[82] Pawlak & Biersteker, *op. cit.*, p. 36.
[83] Giantas & Liaropoulos, *op. cit.*, p. 25.

considered a sensitive area with classified data where information-sharing and exchange of good practices do not come spontaneously.[84] This lack of mutual trust pushes EU member states to tackle cyber-issues on their own rather than conceive it as an EU competence.[85] Moreover, the roots of different policy priorities are not only divergent political preferences, but also a 'cyber-capabilities gap' among member states. The EU includes countries both highly committed to meeting cybersecurity requirements and others being less advanced.[86] Moreover, the immediate political attention of national decision-makers tends to be short lived: while a cyber-attack drives decision-makers to act, engagement at the EU level takes time, meaning that the topic is likely to drop from the national political radar.[87] Finally, some countries cast doubt on ENISA's capacities and may even regard other international frameworks such as NATO or sub-regional cooperation as better equipped to safeguard their security.[88]

Assessment: an orchestra with distinct singers but one voice

Coherence between member states and the EU in cyber-related matters faces many hurdles. In spite of the EU's struggle to shape a more collective approach to cyber-issues, national efforts have not been sufficient.[89] This "mismatch between needs and responses" further contributes to the idea that the EU is not yet a collective cyber-actor.[90] However, these issues are innate to any topic associated with security or defence matters within the EU, as domestically driven approaches reflecting national preferences always result in fragmentation.[91] It would be unjustified not to laud the EU's improvements over the past years, especially because cyber is a fresh area. To tackle the discrepancies, the EU has shown a slow but concrete maturing, trying to make member states converge towards a more synchronised ensemble. The EU rapidly recognised that cyberspace remained a national prerogative, and adopted the role to facilitate coordination and to ensure consistency across national governments.[92] This explains thus the rationale behind the perception of cybersecurity

[84] Carrapico & Barrinha, *op. cit.*, p. 1264.
[85] Giantas & Liaropoulos, *op. cit.*, p. 11.
[86] International Telecommunications Union, *Global Cybersecurity Index (GCI)*, 2018.
[87] Ivan, *op. cit.*, p. 9.
[88] Carrapico & Barrinha, *op. cit.*, p. 1264.
[89] Giantas & Liaropoulos, *op. cit.*, p. 14.
[90] Barrinha & Carrapico, 2018, *op. cit.*
[91] Pawlak & Biersteker, *op. cit.*, p. 28.
[92] Carrapico & Barrinha, *op. cit.*, pp. 1266-1267.

as a "policy field that is considered to represent one of the main successes in security coherence".[93]

Moreover, cyber-crises have encouraged national decision-makers to cooperate more closely and to become more involved in common EU approaches.[94] In the aftermath of cyber-attacks, the emergency of the situation and the fact that it takes time to develop European strategies explain why stronger responses have first flourished at national levels. Member states acknowledged that desirable results might best be achieved at the EU level and have "progressed beyond a 'thin' version to imbue the EU with autonomy".[95] These signs of commitment have led to the EU Cyber-DT, a framework to address malicious cyber-activities within the Common Foreign and Security Policy. This is a clear "demonstration of encouraged cooperation, greater matchmaking of interests and goals among the EU countries".[96]

The EU seeks to provide a long-term response, while it leverages national assets to react quickly and flexibly to imminent threats. This move is symbolised by the NIS Directive, which requests each member state to properly develop its own national cybersecurity strategy, with the tacit purpose to strengthen the overall level of cybersecurity of the Union. Christou summarises this paradox lying in the vertical axis of coherence scrutinised here:

> The EU remains anchored to an aggregating function in that the Member States retain important national prerogatives in cyberspace, but aggregation has meant a significant movement toward EU autonomy.[97]

The EU has developed a decentralised 'asymmetric governance', in order to circumvent its inherent weaknesses and to increase coherence. Coupled with its ability to build resilience, it allows the EU to eventually become a global cyber-power.

The last two sections have demonstrated that the EU is certainly a regional cyber-power. Since the EU is striving to become a powerful global diplomatic actor, it does have the ambition to strengthen its role abroad as a cyber-player able to respond to crises, to promote its vision, to spread its values and norms, and to protect its interests and those of its partners. The EU has broadened its political agenda to embrace cyberspace as a major foreign policy area, modelling in turn new international policy

[93] *Ibid*., p. 1259.
[94] Barrinha & Carrapico, 2018, *op. cit.*
[95] Christou, 2018, *op. cit.*, p. 288.
[96] Giantas & Liaropoulos, *op. cit.*, p. 21.
[97] Christou, 2018, *op. cit.*, p. 294.

objectives.[98] The challenge is to translate all of these provisions into efficient foreign policy instruments. The presence of both domestic capabilities (resilience and coherence) constitutes a fertile ground for the EU's actorness externally. The following sections analyse the projection of the EU's capabilities on the international stage based on two criteria: the EU's responsiveness and attractiveness.

The EU's attractiveness: shaping a 'collective immunity' in cyberspace

Over the last years, cyber-issues have gained increasing traction on the international agenda. The EU placed the establishment of a "coherent international cyberspace policy" among its main priorities.[99] The adoption of European Council conclusions on 'cyber-diplomacy' in 2015 marked the starting point of a "proactive role of the EU in international cyberspace policy-making".[100] Its main purpose is to promote "a global, open, free, stable and secure cyberspace where human rights and fundamental freedoms and the rule of law fully apply".[101] Linked to its ambition to become an international diplomatic and security actor, the EU sought to establish strong multilateral and bilateral networks, deepen strategic partnerships with other cyber-players, and heighten the cyber-resilience in and cyber-capacities of third countries. In turn, this attractiveness, combined with a 'normative magnetism', that is inducing progressively third countries to conform to European norms, could lead to the recognition, acceptance and authority of the EU as a global cyber-actor.

Multilateralism: establishing an active EU-wide position in cyberspace

The EU prioritised "the crafting of collective efforts and multilateral instruments" to strengthen global cyber-resilience and to promote global norms and practices in cyberspace.[102] It has sought to enhance ties with international and regional organisations.[103] Since many of these bodies "favour a more positive agenda in cyberspace [...], the EU could use its established cooperation channels" to include cyber-aspects and project its norms and values.[104]

---

[98] Renard & Barrinha, *op. cit.*, pp. 186-187.
[99] European Commission & High Representative, JOIN(2013) 1 final, *op. cit.*, pp. 14-16.
[100] T. Renard, "EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain", *European Politics and* Society, vol. 19, no. 3, 2018, p. 324.
[101] Council of the EU, *Narrative Paper on an open, free, stable and secure cyberspace in the context of international security*, 9764/1/19 REV 1, Brussels, 5 June 2019, p. 2.
[102] Renard, 2018, *op. cit.*, p. 331.
[103] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 113.
[104] Pawlak, Tikk & Kerttunen, *op. cit.*, p. 7.

The EU draws on multilateral instruments to indirectly promote its values and norms, as well as to enhance international cooperation and mutual assistance. It is worth analysing the EU's reliance on the Council of Europe's Budapest Convention, the "most far-reaching multilateral agreement on cybercrime".[105] As the only binding international agreement on cybersecurity, the EU considers it "a useful instrument for the global promotion of European norms".[106] The 2013 EUCSS put forward the concept of 'cybercrime' alongside 'cybersecurity' to link actions to the Budapest Convention while the 2017 EUCSS refers to the Convention as "the model for drafting national cyber-crime legislation and [...] for international cooperation".[107] For instance, the EU has made its financial support for cyber-capacity building in third countries conditional upon their compliance with the Convention.[108] In addition, the EU considers some international organisations as crucial platforms. It has seen the possibility to build a fruitful complementarity with NATO in fostering its cyber-defence posture, mainly through the collaborative development of resilience capabilities.[109] NATO is the only international organisation whose cooperation with the EU is explicitly highlighted in the 2017 EUCSS.[110] Since 2010 both entities have established regular informal staff-to-staff consultation on cyber-issues or synchronised cyber-exercises.[111] The deepening of the strategic relationship with NATO was initiated in 2016 with "one of the most prominent cyber-cooperation schemes".[112]

Enhancing cooperation in cyberspace through bilateral strategic partnerships

Multilateral ties allow the EU to project its own vision internationally and to shape cyberspace by forging a consensual response to cyber-threats. However, since the "multilateral fabric is particularly thin in [this] policy area, bilateral cooperation appears necessary to palliate and, eventually, strengthen multilateral instruments".[113] The 2013 EUCSS and the 2015 Council conclusions called for an "increased engagement and stronger relations with key international partners".[114] The 2016 EUGS

[105] Fahey, *op. cit.*, p. 48.
[106] Renard, 2018, *op. cit.*, p. 331.
[107] Fahey, *op. cit.*, pp. 47-50.
[108] Renard, 2018, *op. cit.*, p. 331.
[109] P. Pawlak, "Cyber Resilience", in F. Gaub & N. Popescu, *After the EU Global Strategy – Building Resilience*, European Union Institute for Security Studies, Paris, 2017, p. 19.
[110] European Commission & High Representative, JOIN(2017) 450 final, *op. cit.*, pp. 19-20.
[111] Renard, 2018, *op. cit.*, p. 332.
[112] Giantas & Liaropoulos, *op. cit.*, p. 21.
[113] Renard, 2018, *op. cit.*, p. 334.
[114] European Commission & High Representative, JOIN(2013) 1 final, *op. cit.*, p. 14; Council of the EU, "Council conclusions on Cyber Diplomacy", *op. cit.*, pp. 11-12.

stressed the need for the EU to "enhance its cybersecurity with core partners" while the 2017 EUCSS underlines the need to "step up dialogues with third countries to promote global convergence and responsible behaviour in this area".[115]

To shape Internet governance with 'like-minded' partners, the EU "has managed to assert itself as a worthwhile interlocutor in the cyber-domain with all its strategic partners [...] embedding them in a network of dialogues, joint statements and common initiatives".[116] Gradually incorporating cyber-issues into the cooperation agenda, the EU has formalised a "network of bilateral strategic partnerships" with key cyber-actors which is devoted to cooperation, information-sharing, the exchange of best practices and expertise, and confidence-building measures.[117] It first inserted cyber-issues into pre-existing dialogues but rapidly acknowledged the need to launch specific cyber-dialogues on a bilateral level. There is now "at least one dialogue on cyber-related issues with each of the EU's ten strategic partners" (see Figure 2).[118] Among them, the EU-US Cyber Dialogue is the institutionally most developed and the most ambitious, and it is the only one covering "triangulated efforts for cyber-capacity building in third countries".[119] Moreover, the "rule-making in the areas of cybercrime and cybersecurity between the EU and the US constitutes the first major transatlantic cooperation in security since a decade".[120] The EU may also attempt to cement a strategic cyber-partnership with the United Kingdom, as "Brexit will leave a significant gap in the EU's cyber-capabilities".[121]

Figure 2 – EU cyber-dialogues with strategic partners

Partner country	Relevant dialogues
Brazil	Dialogue on international cyber policy; Information society dialogue
Canada	EU-US-Canada Expert Meeting on Critical Infrastructure Protection
China	Cyber taskforce; Dialogue on IT, telecommunications and informatisation
India	Political dialogue on cyber-security; Information society dialogue
Japan	Cyber dialogue; Dialogue on ICT policy
Mexico	Working Group on telecommunications; Dialogue on public security and law enforcement
Russia	Information society dialogue
South Africa	Information society dialogue
South Korea	Cyber dialogue; Information society dialogue
USA	Working Group on Cyber-security and Cyber-crime (WGCC); Cyber dialogue; Information society dialogue; EU-US-Canada Expert Meeting on Critical Infrastructure Protection

[115] EEAS, EUGS 2016, *op. cit.*, p. 22; European Commission & High Representative, JOIN(2017) 450 final, *op. cit.*, p. 19.
[116] Renard, 2018, *op. cit.*, p. 327.
[117] *Ibid.*, pp. 322, 326.
[118] *Ibid.*, p. 334.
[119] *Ibid.*, p. 328.
[120] Fahey, *op. cit.*, pp. 55-56.
[121] Ivan, *op. cit.*, p. 11.

Source: Renard, 2018, *op. cit.*, p. 329.

Cyberspace represents today an "indicator of the depth of the political/security relation and trust between partners".[122] Conversely, partnerships with cyber-players perceived as threats are less developed. Instead, the EU focused on confidence-building aspects, as it seeks "to keep the dialogue open on contentious issues".[123] For instance, in the case of China, the EU has included chapters on cyber in joint cooperation agendas and established the Sino-European Cyber Dialogue.[124] In EU-Russia relations, Crimea's annexation shattered the potential cooperation on cyber-issues.

Capacity building: durable and sustainable cyber-resilience in third countries

The EU also recognised that capacity building in third countries aimed at enhancing cyber-resilience is crucial to protect its interests and project its values. Whereas the number of Internet users "is expected to reach 4.7 billion by 2025, most of this growth is happening in the developing countries and emerging economies". [125] This technological progress will go hand in hand with higher domestic vulnerabilities and exposition to external cyber-threats if a sufficient degree of resilience is not attained. For the EU, this means that allies, potential economic partners, neighbourhood and candidate countries lacking proper cyber-capabilities might be hugely impacted by malicious activities. This could damage economic development, destabilise the political order and *in fine* escalate the risks in sensitive zones.[126] Consequently, the EU pursues the goal of stepping up cyber-capacity building programmes in partner countries in order to improve their cyber-resilience.[127] The EUGS underlined that the EU "will engage in [...] capacity building with [its] partners".[128] The 2017 EUCSS promoted the creation of a "Capacity Building Network to support third countries' ability to address cyber-threats".[129]

In concrete terms, EU projects and initiatives have spanned the globe, e.g. the CB4Resilience (Capacity Building and Cooperation to enhance Cyber Resilience) and

[122] E. Lannon, "EU Cybersecurity Capacity Building in the Mediterranean and the Middle East", in S. Florensa (ed.), *IEMed Mediterranean Yearbook 2019*, Barcelona, 2020, pp. 243-244.
[123] Renard & Barrinha, *op. cit.*, p. 190.
[124] Renard, 2018, *op. cit.*, p. 329.
[125] P. Pawlak, "EU-India Cooperation on cyber issues: towards pragmatic idealism?", *Istituto Affari Internazionali*, Working paper, vol. 16, no. 36, December 2016, p. 3.
[126] Pawlak, "Cyber Resilience", *op. cit.*, p. 17
[127] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 110.
[128] EEAS, EUGS 2016, *op. cit.*, pp. 23-28, 42.
[129] European Commission & High Representative, JOIN(2017) 450 final, *op. cit.*, pp. 19-20.

the ENCYSEC (Enhancing Cybersecurity) projects.[130] In the framework of the European Neighbourhood Policy, the EU placed "fighting cybercrime" among its prime concerns.[131] For instance, it implemented Technical Assistance and Information Exchange Instruments to assist Ukraine in strengthening its cybersecurity capacity.[132] The EU launched a number of projects in collaboration with the Council of Europe such as the CyberSouth programme which aims at strengthening cyber-capabilities to tackle cybercrime in the Southern neighbourhood (especially Algeria, Jordan, Lebanon, Morocco, and Tunisia), GLACY+ focusing "on supporting countries that may serve as hubs to share their experience within their respective regions", or "iPROCEEDS targeting [...] online crime in South-eastern Europe and Turkey, and "Cybercrime&EAP II and III on international cooperation" in the neighbourhood.[133]

Assessment: fomenting a collective immunity against cyber-threats

The EU promotes a multi-stakeholder model in which a broad international community composed of 'like-minded' partners is in charge of shaping a coherent cyberspace. To strengthen global governance in order to mount the most effective response to address the challenges of cyber-warfare, the EU has spurred international cooperation.[134] It relies on a dense network of key bilateral cyber-partnerships, carefully crafted through regular cyber-dialogues that aim at building mutual confidence and facilitating international consensus at the multilateral level. Moreover, the EU has initiated cooperation with regional and international organisations such as the Council of Europe and NATO to supplement its own approach or to address shortcomings. The EU has also invested in third countries in order to provide them with capacity building to reach a sufficient level of resilience.

This international engagement allows the EU to spread its vision, norms and values abroad. In turn, these ties have stimulated the coherence and "integration process of the EU's cyber-policy [...] and a common European cybersecurity agenda.[135] They represent a springboard to influence international debates and constitute a *conditio sine qua non* to be granted a global strategic status in cyberspace.[136] The EU aims at

[130] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 110.
[131] European Commission & High Representative, *Review of the European Neighbourhood Policy*, JOIN(2015) 50 final, 18 November 2015.
[132] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 110.
[133] Pawlak, "Cyber Resilience", *op. cit.*, pp. 18-19.
[134] Pawlak & Biersteker, *op. cit.*, p. 84.
[135] Giantas & Liaropoulos, *op. cit.*, p. 23.
[136] Renard, *op. cit.*, pp. 325, 334.

sculpting a collective international immunity to enhance the capacity of each actor and stakeholder to prevent malicious cyber-operations and effectively deal with their consequences. In the long run, strengthening the cyber-environment would reduce the destabilisation of the international order by shrinking potential escalations of a conflict.[137] This international posture considerably underpins the EU's cyber-actorness, even if there is still "ample scope for boosting the EU's presence and visibility in the cyber-arena".[138]

To be able to promote its vision of an 'open, safe and secure cyberspace', the EU has not only sought to build international resilience but also to frame a more active resistance against malicious cyber-players. The next section assesses the 'responsiveness' criterion, that is, the EU's ability to mobilise its instruments, mechanisms and resources on the international stage to counter hostile cyber-activities.

The EU's responsiveness: oxymoronic cyber-powers?

Facing the shortcomings of existing muddled international frameworks to set up rules in cyberspace, the EU has moulded its own sanctioning apparatus. But rather than becoming an assertive cyber-player, the EU is using a preventive approach to shape cyber-deterrence which could ultimately make it an international cyber-mediator. In turn, some countries might be inclined to climb in the bandwagon led by the Union by setting up their own sanctioning frameworks. However, this section also draws attention to the pitfalls the EU is either afraid or unable to overcome, such as the challenge of attributing cyber-attacks. Finally, what is overall remarkable is the EU 'paradoxical sleep' in relation to its cyber-sanctions regime.

The blurry international law at the origins of the EU's cyber-sanctions regime

The cyber-sphere is highly contested by a growing number of international cyber-players but remains an under-regulated policy area, "where existing international law, rules and norms are undermined through state practice".[139] The EU's *'cyber-acquis'* clearly signals the normative framework the EU upholds: "a rules-based order based on the application of [existing] international law and adherence to voluntary norms of responsible state behaviour", in accordance with the international consensus built

[137] Pawlak, Tikk & Kerttunen, *op. cit.*, p. 7.
[138] Pawlak & Biersteker, *op. cit.*, p. 96.
[139] *Ibid.*, p. 32.

within the United Nations.[140] However, a formal legal delineation about what would be a 'punishable' behaviour is not established.[141] States' behavioural norms are blurred and views on cyber-governance diverge.[142] Faced with this ambiguity, due to the non-binding nature of norms in cyberspace, the EU established its own mechanism to ensure compliance with existing international law and responsible state behaviour but also to make sure that perpetrators are held accountable: the Cyber-DT for a joint EU diplomatic response to malicious cyber-activities.[143] It encompasses a plethora of diplomatic and operational instruments to "promote responsible behaviour and eradicate impunity in cyberspace": preventive, cooperative, stability, and restrictive measures.[144]

This 'cyber-sanctions regime' aims not only at enhancing cybersecurity within the EU but also at creating a stable international cyberspace.[145] Cyber-sanctions entail three functions: coercion in order to bring about a change of behaviour by the target; the constraint of malicious activities by limiting access to resources; and the signalling of norm preferences and potential consequences both to the target and to the international community.[146] Council Decision 2019/797 and the Council Regulation 2019/796 define the scope that might activate the imposition of sanctions. It embraces "cyber-attacks [...] which constitute an external threat to the Union [...] [or] against third States or international organisations".[147] The idea of 'collective cyber-securitisation' and the 'us against them' vision is reflected here.

Applying the EU's main assets in cyberspace: fostering mediation and magnetism

European policy-makers based the sanctions regime on the assumption that "signalling the likely consequence of a cyber-attack would dissuade potential attackers".[148] The EU's past practice of using restrictive measures to promote its core values tipped the scales in favour of the use of cyber-sanctions to "invariably send

[140] *Ibid.*, p. 28.
[141] Ivan, *op. cit.*, p. 8.
[142] Renard, 2018, *op. cit.*, p. 323.
[143] Pawlak & Biersteker, *op. cit.*, pp. 2, 5, 28, 33, 45.
[144] *Ibid.*, p. 87.
[145] Giantas & Liaropoulos, *op. cit.*, p. 20.
[146] Pawlak & Biersteker, *op. cit.*, pp. 9, 22.
[147] Council of the EU, "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union of its Member States", *OJ*, L129I, 17 May 2019, p. 14; Council of the EU, "Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *OJ*, L129I, 17 May 2019, p. 1.
[148] Pawlak & Biersteker, *op. cit.*, pp. 27-28.

normative signals" rather than as a coercive instrument.[149] Consequently, deterrence and signalling norms preferences are intrinsically bound: cyber-sanctions would have a constructive role in preventing attacks and reducing the risks of conflict escalation. To increase its chances of succeeding, this EU cyber-deterrent and signalling posture might be coupled with preventive diplomacy, a "key component of the EU's DNA".[150] It may further boost the EU's credibility internationally and lead the EU to become a potential mediator in cyber-conflict prevention and de-escalation.

The EU could benefit from its dense network of international cyber-partnerships to promote standards and good practices in cyberspace. A combination of its framework with other sanctions regimes would generate "synergies stemming from joint designations from different countries and regional or international organisations".[151] The EU's regime might serve as a reference that "could inspire other nations to rapidly follow suit [...] and contribute to strengthening global compliance with the existing norms".[152] Approving restrictive measures in support of third countries might also guarantee that EU values and interests are mutually reinforced. In turn, the proliferation of cyber-sanctions regimes within 'like-minded' partners could act as a force multiplier in terms of effectiveness, impact, and symbolic weight (to date, eight non-EU members have aligned with the Council Decision 2019/797).[153] Coupled with some international backup, the EU cyber-sanctions regime could strongly enhance the role of the EU as a global cyber-actor.

The challenge of attribution: a cumbersome decision-making process

The EU has opted for developing the signalling capacities of its sanctions regime to discourage potential norm-violators from committing cyber-attacks. In this regard, the attribution of an attack to an actor – a precondition for addressing effectively malicious cyber-activities – may also have a signalling role. It denotes the "process of tracking, identifying and laying blame on the perpetrator of a cyber-attack".[154] Alongside the principles of necessity and proportionality, attribution is required for granting legality to any cyber-sanction under international law.[155] It is essential since

[149] *Ibid*., pp. 5, 22.
[150] Pawlak, Tikk & Kerttunen, *op. cit.*, p. 6.
[151] Pawlak & Biersteker, *op. cit.*, p. 42.
[152] Moret & Pawlak, *op. cit.*, pp. 2-3.
[153] Pawlak & Biersteker, *op. cit.*, pp. 41, 96.
[154] Ivan, *op. cit.*, p. 13.
[155] Moret & Pawlak, *op. cit.*, p. 3.

the decision to apply targeted sanctions is correlated with the level of reliable evidence and the degree of confidence for attributing a cyber-offence.[156]

However, only a few European governments have already publicly attributed offensive cyber-operations to states, when the EU remained mute on the topic. As an illustration, while several member states assigned responsibility of the 'NotPetya' attack to Russia, the EU only condemned the attacks without a collective attribution.[157] The EU fears that a wrong attribution would damage its credibility as a global cyber-actor.[158] To avoid the 'naming and shaming effect', many measures foreseen in the toolbox do not require a high level of attribution while the cyber-sanctions regime, at the other end of the spectrum, has been conceived to blame individuals or entities but in no case to target states.[159] Still, an EU collective attribution to non-state actors remains a laborious task. Member state governments advocate for preserving confidentiality given that gathering evidence for attribution could compromise sensitive national information.[160] Moreover, they lack the "required cyber- and intelligence capabilities, and the political and administrative processes necessary to properly attribute malicious cyber-incidents".[161] Additionally, member states are often influenced by national considerations, especially when outcomes might have implications for countries they share interests with. Given the EU's fragmented decision-making system, these divergences engender difficulties to reach unanimity, and thus to deploy a common response. So far, the Union has abstained from enlisting any individual or entity.[162]

The European 'paradoxical sleep'

The cyber-sanctions regime, symbolising the EU's potential to become a responsive global cyber-actor, contains many incongruities. As mentioned, the EU could play its diplomatic trump card to act as a global mediator in cyberspace. Nonetheless, this function seems incompatible with the firmer approach – ensuring accountability and enhancing enforcement – adopted with the cyber-sanctions regime, which gives more 'teeth' to the EU.[163] Mediation and attribution are antinomic terms: at the same

[156] Pawlak & Biersteker, *op. cit.*, pp. 52-53.
[157] Ivan, *op. cit.*, pp. 6-7.
[158] Pawlak & Biersteker, *op. cit.*, p. 52.
[159] *Ibid.*, p. 61.
[160] Moret & Pawlak, *op. cit.*, p. 4.
[161] Ivan, *op. cit.*, p. 3.
[162] Pawlak & Biersteker, *op. cit.*, p. 30.
[163] Pawlak, Tikk & Kerttunen, *op. cit.*, p. 6.

time, the EU cannot attribute and endorse the role of a mediator, which is by definition against pointing a finger at any particular side. Furthermore, there is a tension between the EU's ambition to forge deterrence through compelling tools and the tendency to elude the question of attribution. In accordance with the 2016 EUGS – "principled pragmatism will guide our external action"[164] – the adoption of the cyber-sanctions regime is a sign of a more pragmatic stance in the world, reflected in the absence of direct references to values in the legal texts implementing it.[165] This fact spells one major contradiction: the EU relies on its cyber-sanctions regime to forge deterrence but it lacks the courage to attribute any cyber-operation to a potential state perpetrator, out of fear of political, reputational and economic costs and of escalating retaliation. Since "sanctions in the cyber-domain are more likely to deter states, but are less likely to deter individuals from acting in the name of states", how can this deterrence be effective if the EU does not take responsibility?[166] Adopting sanctions might worsen the relationship with the targeted country and entail the risk of reprisal, but would the lack of reaction not be likely to encourage more damaging behaviour?[167]

The responsiveness criterion of the EU's international actorness in cyberspace is imbued with a 'paradoxical sleep': the brain acts, but the body is paralysed. During the night, the EU's creativity process is sharpened. It conceives ambitious scopes of action internationally, and crafts models for effective response to counter cyber-attacks. However, when it awakens, the EU has to face its own contradictions, and is mired in its relative international passivity, torn between the different approaches of its members.

Assessment: an ungovernable universe?

In 2004, the Council affirmed that it "will work to further refine sanctions and to adapt the instrument to the new security environment".[168] The recently designed cyber-sanctions regime fits well with this ambition. It seeks to ensure compliance with international law and to enforce norms of responsible state behaviour in

[164] EEAS, EUGS 2016, *op. cit.*, p. 16.
[165] A. Barrinha, "Cyber warfare and democratic institutions in Europe", *European Security Webinar*, Natolin Security and Defence Society – College of Europe, 4 May 2020.
[166] Pawlak & Biersteker, *op. cit.*, p. 20.
[167] Ivan, *op. cit.*, p. 3.
[168] Council of the EU, *Basic Principles on the Use of Restrictive* Measures, 10198/1/04, 7 June 2004, p. 3.

cyberspace.[169] In this regard, the EU might become a global norm enforcer. Moreover, the EU aims at forging deterrence through the signalling function of its new regime. The combination of these sanctions with conventional diplomatic tools could make the EU a legitimate mediator for conflict prevention in cyberspace.[170] The EU's magnetic attraction could further incite third countries to imitate the European model in implementing this kind of framework.

Nevertheless, there is still a gap between the adoption of the regime and its concrete operationalisation. Attributing cyber-misdemeanour to states deemed responsible remains the sole privilege of member states, while the EU keeps dodging the issue. Paralysed, the cyber-sanctions regime has been caught in dilemmas and paradoxes, eroding the EU's international retort in cyberspace. When it comes to addressing malicious actors in cyberspace, the cyber-powers at the disposal of the EU – deterrence, mediation, magnetism, attribution, sanctions – seem oxymoronic, as they are strongly incompatible. From dream to reality, these tergiversations hamper the EU's action and jeopardises its will to take further steps towards becoming a leading cyber-power in the world.

Conclusion: a 'forward-looking' intergalactic cyber-power?

This paper aimed at figuring out to what extent the EU possesses sufficient capabilities to become a global cyber-power. For that purpose, the study has scrutinised through a kinetic approach four criteria that allow evaluating the EU's international actorness in cyberspace: resilience, coherence, attractiveness, and responsiveness. The EU has evolved from an inward-looking cyber-actor to a globally-oriented one.

First, the multiplication of cyber-attacks has raised awareness about the need to rethink the EU's political orientations. The Manichean perception of cyberspace as a potential nest of threats that could induce irreversible damages led the EU to conceive specialised entities and to establish or toughen legal frameworks in order to shape a "comprehensive and integral cybersecurity strategy [to] mitigate the cyber-threats".[171] It resulted in the creation of a 'collective cyber-securitisation' highlighting the capability of the EU to build inland resilience.

[169] Pawlak & Biersteker, *op. cit.*, pp. 10-14.
[170] Moret & Pawlak, *op. cit.*, p. 4.
[171] Giantas & Liaropoulos, *op. cit.*, p. 6.

Second, this 'collective cyber-securitisation' has enabled the EU "to carry out the functions of security governance", at least regionally. [172] This governance is asymmetrical because member states have been reluctant to give too much power to the supranational body. Yet, this reluctance did not impede the EU from exerting authority and enhancing the overall level of coherence by creating a synergetic approach. The EU has demonstrated that it does "add value in this domain, primarily through bolstering capacities [and] law enforcement cooperation".[173]

Third, the EU has extended its ambition to become a global strategic actor to the cyberspace. The Union's normative role in promoting a rules-based international order and its multilateral and bilateral cyber-engagements abroad allowed it to shape a 'collective immunity' in cyberspace and to gain international recognition as a powerful cyber-actor.

Fourth, at first sight, the cyber-sanctions regime seems to boost the EU's global actorness. Nevertheless, the EU is constrained to play a mediation or advisory role rather than assuming an operational function in cyberspace. Entangled in a 'paradoxical sleep', the EU is devoid of means to fulfil its global ambitions.

There is an incremental looping effect: cyber-crises are a driver leading the EU to become resilient and to improve the vertical coherence between member states and the Union. Hence, the EU, equipped with new capabilities, becomes a stronger international cyber-actor. Recognised as a reliable cyber-partner, its power of attractiveness increases, while its emerging ability to respond to cyber-attacks deters potential malicious enemies. The EU is thus a capable cyber-actor with extensive capacities, does possess the normative stance required to be internationally considered legitimate, and its recognition by other actors as a partner in this field makes the EU a credible cyber-player. However, the EU international 'cyber-power' is still incomplete due to the absence of a common strategic vision for security and defence among its members, distrust regarding information-sharing, cyber-capability disparities, the attribution's puzzle, etc.

The paper argues that, in an alarming cybersecurity environment, the EU is, so far, a regional cyber-power, but it has the potential to become a leading global cyber-power. In order to succeed, it must be able to overcome the constraints that are partly inherent to its nature. Like the Guardians of the Galaxy, the "EU's strength comes from

[172] Christou, 2018, *op. cit.*, p. 294.
[173] Pawlak, "Protecting and defending Europe's cyberspace", *op. cit.*, p. 103.

the qualities and powers of its individual members".[174] The prophecy of a potential 'cyber-apocalypse' crouched in the shadows may urge the member states to transform the Union into a global cyber-hero. In the cyber-galaxy, the EU has become a star but it still cannot shine.

[174] Pawlak & Biersteker, *op. cit.*, p. 3.

Bibliography

Barrinha, Andre & Helena Carrapico, "How coherent is EU cybersecurity policy? ", *EUROPP Blog*, London School of Economics and Political Science, 2018, retrieved 27 April 2020, https://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy

Barrinha, Andre, "Cyber warfare and democratic institutions in Europe", *European Security Webinar*, Natolin Security and Defence Society – College of Europe, 4 May 2020.

Bretherton, Charlotte & John Vogler, *The European Union as a Global* Actor, London, Routledge, 2nd edn., 2006.

Carrapico, Helena & André Barrinha, "The EU as a Coherent (Cyber)Security Actor? ", *Journal of Common Market Studies*, vol. 55, no. 6, 2017, pp. 1254-1272.

Christou, George, "The collective securitisation of cyberspace in the European Union", *West European Politics*, vol. 42, no. 2, 2018, pp. 278-301.

Christou, George, *Cybersecurity in the European Union. Resilience and Adaptability In Governance* Policy, Basingstoke, Palgrave Macmillan, 2016.

Council of the European Union & European Parliament, "Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology cybersecurity certification", *Official Journal of the European Union*, L151, 7 June 2019.

Council of the European Union, "Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union of its Member States", *Official Journal of the European Union*, L129I, 17 May 2019.

Council of the European Union, "Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems", *Official Journal of the European Union*, L69, 16 March 2005.

Council of the European Union, "Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States", *Official Journal of the European Union*, L129I, 17 May 2019.

Council of the European Union, *Basic Principles on the Use of Restrictive Measures*, 10198/1/04, 7 June 2004.

Council of the European Union, *Cybersecurity – Information from the Commission*, 9621/17, Brussels, 31 May 2017.

Council of the European Union, *Internal Security Strategy for the European Union: Towards a European Security Model*, March 2010.

Council of the European Union, *Narrative Paper on an open, free, stable and secure cyberspace in the context of international security*, 9764/1/19 REV 1, Brussels, 5 June 2019.

ENISA, *National Cyber Security Strategies – Interactive Map*, 2020, retrieved on 19 April 2020, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

ENISA, *Overview of cybersecurity and related terminology*, Version 1, September 2017.

ENISA, *WannaCry Ransomware: first ever case of cyber cooperation at EU level*, Press release, 15 May 2017, retrieved 28 April 2020, https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level

European Commission & High Representative, *Joint Communication to the European Parliament and the Council: Strategic Approach to Resilience in the EU's external* action, JOIN(2017) 21 final, Brussels, 7 June 2017.

European Commission & High Representative, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final, Brussels, 7 February 2013.

European Commission & High Representative, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Review of the European Neighbourhood* Policy, JOIN(2015) 50 final, Brussels, 18 November 2015.

European Commission & High Representative, *Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450 final, Brussels, 13 September 2017.

European Commission, *Communication from the Commission to the Council and the European Parliament, Critical Infrastructure Protection in the fight against Terrorism*, COM(2004) 702 final, Brussels, 20 October 2004.

European Commission, *Communication from the Commission to the Council and the European Parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre*, COM(2012) 140 final, Brussels, 28 March 2012.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*, COM(2015) 185 final, Strasbourg, 28 April 2015.

European Council, *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World*, S407/08, Brussels, 11 December 2008.

European External Action Service, *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign And Security Policy*, June 2016.

European Parliament, *Resolution of 24 May 2007 on Estonia*, 2007/2567 (RSP), 27 May 2007.

Fahey, Elaine, "The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation*, vol. 5, no.1, 2014, pp. 46-60.

Fox, Benjamin, "Parliament demands single EU voice on cybersecurity", *EUObserver*, 13 June 2012, retrieved 3 May 2020, https://euobserver.com/creative/116606.

Giantas, Dominika & Andrew Liaropoulos, *Cybersecurity in the EU. Threats, Frameworks and future perspectives*, Working paper, no. 1, Piraeus, Laboratory of Intelligence & Cyber-Security, September 2019.

International Telecommunications Union, *Global Cybersecurity Index (GCI)*, 2018, retrieved 20 April 2020, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Ivan, Paul, *Responding to cyber-attacks: prospects for the EU Cyber Diplomacy Toolbox,* Discussion Paper, European Policy Centre, 18 March 2019.

Krause, Hannes, "How to advance European Cybersecurity? ", *International Centre for Defence and Security, Estonia*, 8 June 2018, retrieved on 18 April 2020, https://icds.ee/how-to-advance-european-cybersecurity/.

Limnell, Jarno, "Russia cyber activities in the EU", in Popescu, Nicu & Stanislav Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018, pp. 65-73.

Moret, Erica & Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: towards a cyber-sanctions regime?*, Brief, no. 24, European Union Institute for Security Studies, Paris, July 2017.

Pawlak, Patryk & Thomas Biersteker, *Guardian of the Galaxy. EU cyber sanctions and norms in cyberspace*, Chaillot Paper, no. 155, European Union Institute for Security Studies, Paris, October 2019.

Pawlak, Patryk, "Cyber Resilience", in Florence Gaub & Nicu Popescu (eds.), *After the EU Global Strategy – Building Resilience*, European Union Institute for Security Studies, Paris, 2017, pp. 17-20.

Pawlak, Patryk, "EU-India Cooperation on cyber issues: towards pragmatic idealism?", *Istituto Affari Internazionali*, Working Paper, vol. 16, no. 36, December 2016.

Pawlak, Patryk, "Protecting and defending Europe's cyberspace", in Popescu, Nicu & Stanislav Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018, pp. 103-114.

Pawlak, Patryk, Eneke Tikk & Mika Kerttunen, "Cyber Conflict Uncoded – The EU and conflict prevention in cyberspace", *Conflict Series Brief*, no. 7, European Union Institute for Security Studies, Paris, April 2020.

Pernik, Piret, "The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine", in Popescu, Nicu & Stanislav Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018, pp. 53-64.

Pospecu, Nicu & Stanislav Secrieru, "Conclusions", in Pospecu, Nicu & Stanislav Secrieru (eds.), *Hacks, leaks and disruptions. Russian cyber strategies*, Chaillot Paper, no. 148, European Union Institute for Security Studies, Paris, October 2018, pp. 115-118.

Rehrl, Jochen, *Handbook on Cybersecurity*, Vienna, Ministry of Defence of Austria, 2018.

Renard, Thomas, "EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain", *European Politics and Society*, vol. 19, no. 3, 2018, pp. 321-337.

Renard, Thomas, "The Rise of Cyber-Diplomacy: the EU, Its Strategic Partners and Cyber-Security", *ESPO Working Paper*, no. 7, European Strategic Partnership Observatory, June 2014.

Ruus, Kertu, "Cyber War I: Estonia Attacked from Russia", *European Affairs*, vol. 9, issue 1-2, 2008.

Saurugger, Sabine & Fabien Terpan, "Explaining the transformation of law. The cases of economic governance, migration and cybersecurity", Paper presented at the EUSA Conference, Denver, May 2019.

Senén, Florensa, *IEMed Mediterranean Yearbook 2019*, Barcelona, 2020.

Sliwinski, Krzystof Feliks, "Moving beyond the European Union's weakness as a cyber-security agent", *Contemporary Security* Policy, vol. 35, no. 3, 2014, pp. 468-486.

Sperling, James & Mark Webber, "The European Union: Security Governance and Collective Securitization", *West European Politics*, vol. 42, no. 2, 2018, pp. 228-260.

Teffer, Peter, "EU Countries miss cybersecurity deadline", *EU Observer*, 30 July 2018, retrieved 22 April 2020, https://euobserver.com/digital/142493.

Tsagourias, Nicholas & Russel Buchan, *Research Handbook on International Law and Cyberspace*, Cheltenham: Edward Elgar Publishing, 2015.

List of recent EU Diplomacy Papers

For the full list of papers and free download, please visit
www.coleurope.eu/EUDP

1/2020
Susanna Garside, *Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom*

2/2020
Sabine Weyand, *A Stronger Europe in the World: Major Challenges for EU Trade Policy*

3/2020
Elene Panchulidze, *Limits of Co-mediation: The EU's Effectiveness in the Geneva International Discussions*

4/2020
Tatiana Kakara, *Mega-regionals and the EU-Japan Economic Partnership Agreement: A Historical Institutionalist Analysis*

5/2020
Adrien Boudet, *Un « triangle d'incompatibilité » ? La relation entre Brexit, défense européenne et PSDC*

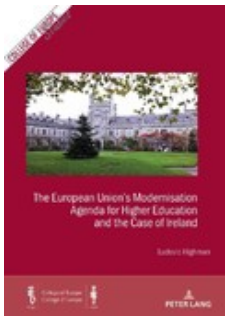
6/2020
Mark Heemskerk, *Bringing Europe to the Western Balkans: The Europeanisation of Croatia and Serbia Compared*

7/2020
Monika de Silva, *Accession of the European Union to the United Nations Human Rights Treaties: Explaining the Reasons for Inaction*

8/2020
Stefania Kolarz, *The European Union's Engagement with the 'de-facto States' in the Eastern Partnership*

9/2020
Stephen Frain, *Leading from Behind: The EU's Normative Power in the Multilateral Promotion of Human Rights in Africa*

1/2021
Constant Pâris, *Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace*



College of Europe Studies

Order online at www.peterlang.com

PIE - Peter Lang Bruxelles

vol. 20 Highman, Ludovic, *The European Union's Modernisation Agenda for Higher Education and the Case of Ireland*, 2017 (272 p.) ISBN 978-2-8076-0616-6 pb.

vol. 19 Bourgeois, Jacques H.J. / Marco Bronckers / Reinhard Quick (eds.), *WTO Dispute Settlement: a Check-up: Time to Take Stock*, 2017 (167 p.) ISBN 978-2-80760-377-6 pb.

vol. 18 Schunz, Simon, *European Union Foreign Policy and the Global Climate Regime*, 2014 (371 p.), ISBN 978-2-87574-134-9 pb.

vol. 17 Govaere, Inge / Hanf, Dominik (eds.), *Scrutinizing Internal and External Dimensions of European Law: Les dimensions internes et externes du droit européen à l'épreuve,* Liber Amicorum Paul Demaret, Vol. I and II, 2013 (880 p.), ISBN 978-2-87574-085-4 pb.

vol. 16 Chang, Michele / Monar, Jörg (eds.), *The European Commission in the Post-Lisbon Era of Crises: Between Political Leadership and Policy Management (With a Foreword by Commission Vice President Maros Sefcovic)*, 2013 (298 p.), ISBN 978-2-87574-028-1 pb.

vol. 15 Mahncke, Dieter / Gstöhl, Sieglinde (eds.), *European Union Diplomacy: Coherence, Unity and Effectiveness (with a Foreword by Herman Van Rompuy)*, 2012 (273 p.), ISBN 978-90-5201-/842-3 pb.

vol. 14 Lannon, Erwan (ed.), *The European Neighbourhood Policy's Challenges / Les défis de la politique européenne de voisinage,* 2012 (491 p.), ISBN 978-90-5201-779-2 pb.

vol. 13 Cremona, Marise / Monar, Jörg / Poli, Sara (eds.), *The External Dimension of the European Union's Area of Freedom, Security and Justice*, 2011 (434 p.), ISBN 978-90-5201-728-0 pb.

vol. 12 Men, Jing / Balducci, Giuseppe (eds.), *Prospects and Challenges for EU-China Relations in the 21st Century: The Partnership and Cooperation Agreement*, 2010 (262 p.), ISBN 978-90-5201-641-2 pb.

vol. 11 Monar, Jörg (ed.), *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*, 2010 (268 p.), ISBN 978-90-5201-615-3 pb.

vol. 10 Hanf, Dominik / Malacek, Klaus / Muir Elise (dir.), *Langues et construction européenne,* 2010 (286 p.), ISBN 978-90-5201-594-1 br.

vol. 9 Pelkmans, Jacques / Hanf, Dominik / Chang, Michele (eds.), *The EU Internal Market in Comparative Perspective: Economic, Political and Legal Analyses*, 2008 (314 p.), ISBN 978-90-5201-424-1 pb.

vol. 8 Govaere, Inge / Ullrich, Hans (eds.), *Intellectual Property, Market Power and the Public Interest*, 2008 (315 p.), ISBN 978-90-5201-422-7 pb.

vol. 7 Inotai, András, *The European Union and Southeastern Europe: Troubled Waters Ahead?*, 2007 (414 p.), ISBN 978-90-5201-071-7 pb.

vol. 6 Govaere, Inge / Ullrich, Hanns (eds.), *Intellectual Property, Public Policy, and International Trade*, 2007 (232 p.), ISBN 978-90-5201-064-9 pb.